Title (en)

DETECTING AND COUNTERING MALICIOUS CODE IN ENTERPRISE NETWORKS

Title (de)

FESTSTELLUNG UND VERHINDERUNG VON BÖSWILLIGEM RECHNERKODE IN EINEM FIRMENNETZWERK

Title (fr)

DETECTION ET NEUTRALISATION DE CODE MALVEILLANT DANS DES RESEAUX D'ENTREPRISE

Publication

EP 1495616 B1 20100505 (EN)

Application

EP 03719797 A 20030415

Priority

- US 0311824 W 20030415
- US 37313502 P 20020417

Abstract (en)

[origin: US2003200464A1] A system and method for detecting and countering malicious code in an enterprise network are provided. A pattern recognition processor monitors local operations on a plurality of local machines connected through an enterprise network, to detect irregular local behavior patterns. An alert may be generated after an irregularity in behavior pattern on a local machine is detected. Irregular behavior alerts from a plurality of local machines are analyzed. If similar alerts are received from at least a threshold number of local machines over a corresponding period of time, one or more countermeasure operations are selected based on the analysis of the irregular behavior alerts. The selected countermeasure operations are communicated to the local machines and performed by the local machines.

IPC 8 full level

G06F 21/56 (2013.01); **H04L 29/06** (2006.01); **G06F 13/00** (2006.01); **G06F 15/00** (2006.01); **H04L 12/66** (2006.01)

CPC (source: EP KR US)

G06F 11/30 (2013.01 - KR); **G06F 15/00** (2013.01 - KR); **G06F 15/173** (2013.01 - KR); **H04L 63/0218** (2013.01 - EP US); **H04L 63/145** (2013.01 - EP US)

Citation (examination)

US 6088804 A 20000711 - HILL DOUGLAS W [US], et al

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

DOCDB simple family (publication)

US 2003200464 A1 20031023; **US 7934103 B2 20110426**; AT E467297 T1 20100515; AU 2003223656 A1 20031103; BR 0309288 A 20050209; CA 2480475 A1 20031030; CN 1647483 A 20050727; DE 60332448 D1 20100617; EP 1495616 A1 20050112; EP 1495616 B1 20100505; IL 164609 A0 20051218; JP 2005523539 A 20050804; KR 20040101490 A 20041202; WO 03090426 A1 20031030

DOCDB simple family (application)

US 41411703 A 20030415; AT 03719797 T 20030415; AU 2003223656 A 20030415; BR 0309288 A 20030415; CA 2480475 A 20030415; CN 03808403 A 20030415; DE 60332448 T 20030415; EP 03719797 A 20030415; IL 16460904 A 20041014; JP 2003587076 A 20030415; KR 20047016497 A 20030415; US 0311824 W 20030415